Electronic Version
Stylesheet Version v1.1.1

Claims

[c1] 1. A method for a transaction source and a transaction target to exchange a transaction that cannot be repudiated, the method comprising:

(a) receiving a first request for a transaction identifier to identify the transaction, wherein said request includes a source authentication assertion;

(b) verifying said source authentication assertion;

(c) storing said transaction identifier and information from said source authentication assertion, thereby establishing information making the transaction source unable to plausibly repudiate once it encrypts and sends the transaction;

(d) providing said transaction identifier in reply to said first request so that the transaction and said transaction identifier can be sent to the transaction target;

(e) receiving a second request for a decryption key to decrypt the transaction once it has been received by the transaction target, wherein said second request includes said transaction identifier and a target authentication assertion;

(f) verifying said target authentication assertion;

(g) storing information from said target authentication assertion with the transaction identifier; and

(h) providing said decryption key in reply to said second request so that the transaction can be decrypted, thereby establishing information making the transaction target unable to plausibly repudiate being a recipient of the transaction.

[c2] 2. The method of claim 1, wherein said step (d) includes also providing an encryption key to encrypt the transaction.

[c3] 3. The method of claim 1, the method further comprising:

(i) receiving an information request for source information about the transaction source, wherein said information request includes said transaction identifier;

(j) retrieving at least some of said information from said source authentication assertion stored in said step (c) with said transaction identifier and determining said source information therefrom; and

(k) providing said source information in reply to said information request.

[c4] 4. The method of claim 1, the method further comprising:

(i) receiving an information request for target information, wherein said information request includes said transaction identifier and information identifying the transaction target;

(j) determining if said information identifying the transaction target matches with any said information from said target authentication assertion stored with the transaction identifier stored in said step (g) and determining said target information therefrom; and

(k) providing said target information in reply to said information request.

[c5] 5. A method for establishing a transaction as nonrepudiate able by a transaction source that is the origin of the transaction, the method comprising:

(a) receiving a request for a transaction identifier to identify the transaction, wherein said request includes a source authentication assertion;

(b) verifying said source authentication assertion;

(c) storing said transaction identifier and information from said source authentication assertion; and

(d) providing said transaction identifier in reply to said request, thereby establishing information making the transaction source unable to plausibly repudiate being the origin of the transaction.

[c6] 6. The method of claim 5, wherein said step (d) includes also providing an encryption key to encrypt the transaction.

[c7] 7. The method of claim 5, the method further comprising:

(e) receiving an information request for source information about the transaction source, wherein said information request includes said transaction identifier;

(f) retrieving at least some of said information from said source authentication assertion stored in said step (c) with said transaction identifier and determining said source information therefrom; and

(g) providing said source information in reply to said information request.

[c8] 8. The method of claim 7, wherein said source information indicates who the transaction source actually is.

[c9] 9. The method of claim 7, wherein:

said information request received in said step (e) also includes information identifying a party believed to be the transaction source; and

said source information provided in said step (g) indicates merely whether said party is the transaction source, thereby responding to said information re-

quest without specifically identifying the transaction source.

[c10] 10. The method of claim 7, wherein:
said step (c) includes also storing a decryption key usable to decrypt the transaction; and
said step (g) includes also providing said decryption key, thereby facilitating decryption of the transaction by a party making said information request even when said party is not the transaction source or a target of the transaction.

[c11] 11. The method of claim 7, wherein:
said information request received in said step (e) also includes the transaction; and
said step (g) includes decrypting the transaction before providing said source information in reply to said information request.

[c12] 12. The method of claim 11, wherein:
said information request received in said step (e) also includes information identifying a party believed to be the transaction source; and
said source information provided in said step (g) indicates merely whether said party is the transaction source, thereby responding to the second request without specifically identifying the transaction

source.

[c13] 13. The method of claim 11, wherein said step (g) includes also providing the transaction in decrypted form in said reply to said information request, thereby facilitating a party making said information request being able to confirm the content of the transaction even when said party is not the transaction source or a target of the transaction.

[c14] 14. A method for establishing a transaction as nonrepudiate able by a transaction target that is a recipient of the transaction, wherein a transaction identifier identifying the transaction and a decryption key usable to decrypt the transaction have been pre-stored, the method comprising:

(a) receiving a request for the decryption key, wherein said request includes the transaction identifier and a target authentication assertion;

(b) verifying said target authentication assertion;

(c) storing information from said target authentication assertion with the transaction identifier; and

(d) providing the decryption key in reply to said request, thereby establishing information making the transaction target unable to plausibly repudiate being a recipient of the transaction.

[c15] 15. The method of claim 14, the method further comprising:

(e) receiving an information request for target information, wherein said information request includes said transaction identifier and information identifying the transaction target;

(f) retrieving at least some of said information from said target authentication assertion stored in said step (c) with said transaction identifier and determining said target information therefrom; and

(g) providing said target information in reply to said information request.

[c16] 16. The method of claim 15, wherein:

said step (g) includes also providing said decryption key, thereby facilitating decryption of the transaction by a party making said information request even when said party is not the transaction source or a transaction target.

[c17] 17. The method of claim 15, wherein:

said information request received in said step (e) also includes the transaction; and

said step (g) includes decrypting the transaction before providing said identity information.

[c18] 18. The method of claim 17, wherein said step (g) in-

cludes also providing the transaction in decrypted form in said reply to said information request, thereby facilitating a party making said information request being able to confirm the content of the transaction even when said party is not the transaction source or a transaction target.

[c19] 19. A system for a transaction source and a transaction target to exchange a transaction that cannot be repudiated, comprising:

a computerized key server;

said key server suitable for receiving a first request via a network for a transaction identifier to identify the transaction, wherein said first request includes a source authentication assertion;

said key server suitable for receiving a second request via said network for a decryption key usable to decrypt the transaction, wherein said second request includes said transaction identifier and a target authentication assertion;

said key server suitable for verifying said source authentication assertion and said target authentication assertion;

said key server suitable for storing said transaction identifier, information from said source authentication assertion, and information from said target au-

thentication in association in a database;

said key server suitable for providing a first reply to said first request via said network that includes said transaction identifier; and

said key server suitable for providing a second reply to said second request via said network that includes said decryption key, thereby establishing information making the transaction source unable to plausibly repudiate once it encrypts and sends the transaction and also making the transaction target unable to plausibly repudiate once it is provided said decryption key.

[c20] 20. The system of claim 19, wherein said key server is further suitable for providing an encryption key to encrypt the transaction in said first reply.

[c21] 21. The system of claim 19, wherein:

said key server is further suitable for receiving an information request for source information about the transaction source, wherein said information request includes said transaction identifier;

said key server is further suitable for retrieving said information from said source authentication assertion stored with said transaction identifier from said database and determining said source information therefrom; and

said key server is further suitable for providing said source information in reply to said information request.

[c22] 22. The system of claim 19, wherein:

said key server is further suitable for receiving an information request for target, wherein said information request includes said transaction identifier and information identifying the transaction target;

said key server is further suitable for determining if said information identifying the transaction target matches with any said information from said target authentication assertion stored with the transaction identifier and determining said target information therefrom; and

said key server is further suitable for providing said target information in reply to said information request.

[c23] 23. A system for establishing a transaction as nonrepudiate able by a transaction source that is the origin of the transaction, comprising:

a computerized key server;

said key server suitable for receiving a request via a network for a transaction identifier to identify the transaction, wherein said request includes a source authentication assertion;

said key server suitable for verifying said source authentication assertion;

said key server suitable for storing said transaction identifier and information from said source authentication assertion in a database; and

said key server suitable for providing a reply via said network that includes said transaction identifier, thereby establishing information making the transaction source unable to plausibly repudiate once it encrypts and sends the transaction.

[c24] 24. The system of claim 23, wherein said key server is further suitable for providing an encryption key to encrypt the transaction in said reply.

[c25] 25. The system of claim 23, wherein:

said key server is further suitable for receiving an information request for source information about the transaction source, wherein said information request includes said transaction identifier;

said key server is further suitable for retrieving information from said source authentication assertion stored with said transaction identifier from said database, and determining said source information therefrom; and

said key server is further suitable for providing said source information in reply to said information re-

quest.

[c26] 26. A system for establishing a transaction as nonrepudiate able by a transaction target that is a recipient of the transaction, wherein a transaction identifier identifying the transaction and a decryption key usable to decrypt the transaction have been pre-stored in a database, comprising:

a computerized key server;

said key server suitable for receiving a request via a network for the decryption key, wherein said request includes the transaction identifier and a target authentication assertion;

said key server suitable for verifying said target authentication assertion;

said key server suitable for storing information from said target authentication assertion with the transaction identifier in the database; and

said key server suitable for providing a reply via said network that includes the decryption key, thereby establishing information making the transaction target unable to plausibly repudiate.

[c27] 27. The system of claim 26, wherein:

said key server is further suitable for receiving an information request for target information, wherein said information request includes said transaction

identifier and information identifying the transaction target;

said key server is further suitable for retrieving at least some of said information from said target authentication assertion stored with said transaction identifier and determining said target information therefrom; and

said key server is further suitable for providing said target information in reply to said information request.